Technology Management Mistakes

Top 10 Things SMBs Must Consider and Avoid

Small and medium businesses focus on understanding all they can in order to identify and exploit opportunity in the market. Doing so makes sense as the business seeks new revenue and profit.

Unfortunately, small and medium businesses don't have the same focus in their adoption, integration and management of technology. Most often SMBs take a reactionary approach to their technology – creating disruption and additional cost to the business.

Avoid falling into this trap by understanding and working towards overcoming the following common mistakes:

- Weak Internal Technical Support: Often technical support is assigned to the employee who is the 'computer geek'-type. They perform these duties in addition to their regular job responsibilities, often leading to poor performance and results in both areas.

- Keeping Older Technology Too Long: It is a well known fact that older technology needs more repair and fails more often – leading to business downtime. It doesn't accommodate new, lower cost features and functions designed to increase productivity and lower expense.

- Not Keeping Software Licenses Current: When a business doesn't keep their software licenses current they miss out on critical updates, don't have access to technical support and hold their people back from being as productive as possible.

- Training as a Last Resort: SMBs often assume an employee knows how to use the technology or that the employee will 'figure it out.' Instead, you should offer training to your users as a mechanism to increase productivity – especially when you introduce new technology or applications.

- Poor Technology or Information Security: Most businesses use passwords to access networks and email. But, often they don't have policies or tools to ensure the right level of information and technology security needed to adequately protect the business from external intrusion, theft, or disaster recovery.

- Sporadic Data Backup: Many SMBs back up their critical applications and information right after they had a failure. At this point, it is too late. Having the right policies and tools to regularly backup business information will keep you out of future trouble.

- Inadequate Virus/Spam Protection: Viruses and spam represent a large problem for SMBs. Both rob the business of productivity, time and money. SMBs must go beyond simple PC-based tools to ensure the best protection of your systems, information, people and budget.

- Allowing "Personal" Applications on Business Equipment: Because most SMBs don't manage their technology, individual employees are free to add their own personal pictures, software, games, and information – often leading to poorly performing systems and security breaches.

- Open Wireless Networks: With the ease and proliferation of wireless networking, many SMBs accidentally leave their wireless access points open and available for anyone to access. This huge vulnerability puts your systems, information and business at risk.

- No Laptop Security: As employees work at home or travel, they take critical business information with them. SMBs often forget to encrypt or protect critical information from accidental theft or loss when the laptop is lost or stolen.

Your business can easily and quickly eliminate each of these problems with the SMB IT Manager, from NextCorp. As a fully turnkey IT management service, the SMB IT Manager ensures that your technology is always managed, secured and optimized for the greatest productivity and business protection.

Discover how you can overcome these challenges with the SMB IT Manager by simply visiting **www.smbsuite.com** or by calling 1-**800-525-NEXT**. Best in class and cost effective technology management is one call or click away! Go ahead. You have nothing to lose and everything to gain!